Universidade Federal de Uberlândia - UFU
Prof. Rodrigo Sanches Miani

Atividade 4 – Criptografia assimétrica

Objetivo: Familiarizar os alunos com os conceitos de criptografia assimétrica, em particular o algoritmo RSA.

Tarefas

1. Criação de chaves pública/privada.
    a. Use o openssl para criar um par de chaves pública/privada para o algoritmo RSA com 2048 bits.
    b. É possível proteger a chave privada gerada com algum mecanismo de segurança? Se sim, mostre como.
    c. Abra o arquivo referente a chave pública. Que tipo de codificação foi usada no conteúdo do arquivo?
    d. Após descobrir o tipo de codificação e conseguir ler o arquivo, mostre o valor do par (n,e) da sua chave pública. Qual o tamanho de n (número de digitos)?
    e. Implemente, ou use, um algoritmo qualquer disponível online (https://www.alpertron.com.ar/ECM.HTM) para verificar até que ponto a fatoração de n é possível. Por exemplo, selecione os 10 primeiros dígitos de n, e tente fatorar. Selecione os 20 primeiros e assim por diante. Qual foi o último tamanho possível de fatoração? Qual a relação disso com a segurança do RSA?
    f. Crie um documento com o seu nome e número de matrícula e cifre/decifre tal documento usando a implementação do RSA fornecida pelo *openssl* com a chave criada na letra a). Existe alguma limitação no tamanho do arquivo/mensagem que será cifrada? Faça um paralelo com as implementações de algoritmos simétricos.
2. Use o comando "*speed*" do *openssl* para criar uma comparação de desempenho entre o RSA x DES x 3DES. O desempenho dos algoritmos está em consonância com o que foi estudado durante a disciplina?
3. Pesquise e explique como algoritmos assimétricos, como o RSA, convertem texto em números para realizar as operações de cifrar/decifrar.
4. Pesquise e explique a importância do *padding* para criptografia assimétrica, em particular para o RSA. Qual método de *padding* é usado no RSA?